

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-340579

(43)Date of publication of application : 24.12.1996

(51)Int.Cl.

H04Q 7/38  
H04M 1/66

(21)Application number : 07-144855

(71)Applicant : SONY CORP

(22)Date of filing : 12.06.1995

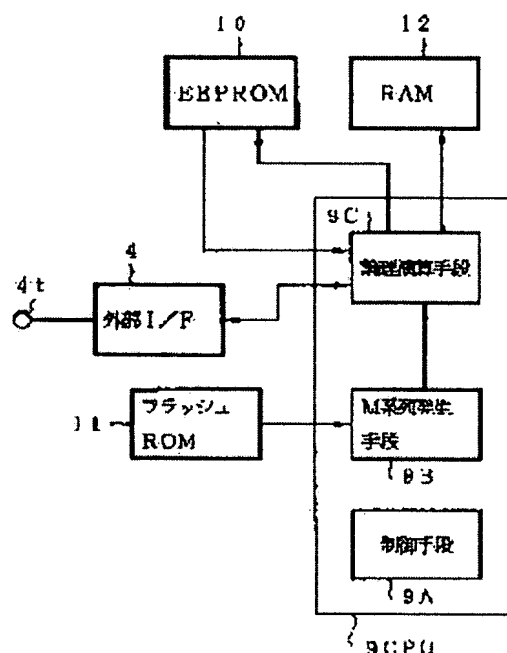
(72)Inventor : SOMEYA MASAHIKA

## (54) PORTABLE TELEPHONE SET

## (57)Abstract:

**PURPOSE:** To prevent illegal use by obtaining scrambled identification information in a RAM by conducting a prescribed arithmetic operation between scrambled identification information read from the RAM and a scrambled code.

**CONSTITUTION:** At application of power, a default of a scramble code stored in a flush ROM 11 is read by a control means 9A. The default is fed to an M series generating means 9B of a CPU 9 to allow the means 9B to generate a 16-bit scramble code updated for each two bytes of identification information. Based on control by the means 9A, the scramble code updated for each 2-byte and an identification information part for each 2-byte of the identification information are exclusively ORed to conduct descrambling and the result is written in a volatile RAM 12. Furthermore, in the case of calling, based on the control by the means 9A, the identification information stored in the RAM 12 is read and fed to a radio section, from which the information is sent.



## LEGAL STATUS

[Date of request for examination] 28.03.2001

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3404993

[Date of registration] 07.03.2003

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平8-340579

(43) 公開日 平成8年(1996)12月24日

(51) Int.Cl. <sup>6</sup>	識別記号	庁内整理番号	F I	技術表示箇所	
H 0 4 Q	7/38		H 0 4 B	7/26	1 0 9 R
H 0 4 M	1/66		H 0 4 M	1/66	A

審査請求 未請求 請求項の数 1 O L (全 5 頁)

(21) 出願番号 特願平7-144855

(22) 出願日 平成7年(1995)6月12日

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 染谷 賢久

東京都品川区北品川6丁目7番35号 ソニー株式会社内

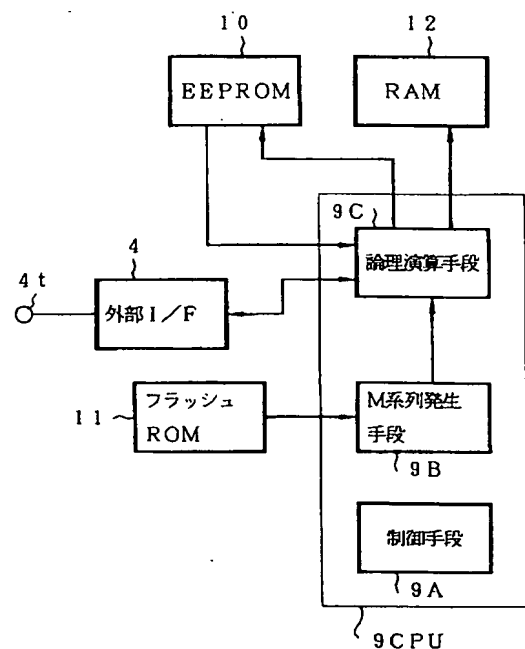
(74) 代理人 弁理士 松隈 秀盛

(54) 【発明の名称】 携帯電話機

(57) 【要約】 (修正有)

【目的】 盗用されることを防止する。

【構成】 制御手段9は、ROM11に製造時に予め記憶されたスクランブルコードの製品毎に異なる初期値から順次変化するスクランブルコードを発生するスクランブルコード発生手段9Bと、外部からの識別情報及びスクランブルコード発生手段9Bよりのスクランブルコードの間で所定の論理演算を行って、不揮発性RAMに書き込むためのスクランブルされた識別情報を得ると共に、不揮発性RAM10から読み出されたスクランブルされた識別情報及びスクランブルコード発生手段9Bよりのスクランブルコードの間で所定の論理演算を行って、揮発性RAM12に書き込むためのデスクランブルされた識別情報を得る論理演算手段9Cとを備える



C P U の 機 能 ブ ロ ッ ク

1

## 【特許請求の範囲】

【請求項 1】 スランブルされた識別情報を記憶する不揮発性 RAM と、スランブルコードの製品毎に異なる初期値が製造時に予め記憶された ROM と、デスクランブルされた識別情報を記憶する揮発性 RAM と、上記不揮発性 RAM、上記 ROM 及び上記揮発性 RAM を制御する制御手段とを有し、

該制御手段は、

上記 ROM に記憶されているスランブルコードの初期値から順次変化するスランブルコードを発生するスランブルコード発生手段と、

外部からの識別情報及び上記スランブルコード発生手段よりのスランブルコードの間で所定の論理演算を行って、上記不揮発性 RAM に書き込むためのスランブルされた識別情報を得ると共に、上記不揮発性 RAM から読み出されたスランブルされた識別情報及び上記スランブルコード発生手段よりのスランブルコードの間で所定の論理演算を行って、上記揮発性 RAM に書き込むためのデスクランブルされた識別情報を得る論理演算手段とを備えることを特徴とする携帯電話機。

## 【発明の詳細な説明】

## 【0001】

【産業上の利用分野】 本発明は携帯電話機に関する。

## 【0002】

【従来の技術】 従来の携帯電話機では、加入者番号、移動局番号、認証及び秘匿のキー等を含む識別情報がスランブルコードによってスランブルされ、そのスランブルされた識別情報が、CPU を含んだ制御部の不揮発性 RAM に記憶され、そのスランブルコードの初期値が、その制御部の ROM に記憶されると共に、その制御部にそのスランブルコードを発生するアルゴリズムが設けられていた。

## 【0003】

【発明が解決しようとする課題】 かかる従来の携帯電話機では、制御部の ROM に記憶されているスランブルコードの初期値が、製品毎に共通であったため、制御部の記憶内容やアルゴリズムを別の携帯電話機の制御部にコピーして、実質的に他人の携帯電話機を盗用することは容易であった。

【0004】 かかる点に鑑み、本発明は、実質的に他人の携帯電話機を盗用することを防止することのできる携帯電話機を提案しようとするものである。

## 【0005】

【課題を解決するための手段】 本発明による携帯電話機は、スランブルされた識別情報を記憶する不揮発性 RAM と、スランブルコードの製品毎に異なる初期値が製造時に予め記憶された ROM と、デスクランブルされた識別情報を記憶する揮発性 RAM と、不揮発性 RAM、ROM 及び揮発性 RAM を制御する制御手段とを有し、その制御手段は、ROM に記憶されているスラン

2

ブルコードの初期値から順次変化するスランブルコードを発生するスランブルコード発生手段と、外部からの識別情報及びスランブルコード発生手段よりのスランブルコードの間で所定の論理演算を行って、不揮発性 RAM に書き込むためのスランブルされた識別情報を得ると共に、不揮発性 RAM から読み出されたスランブルされた識別情報及びスランブルコード発生手段よりのスランブルコードの間で所定の論理演算を行って、揮発性 RAM に書き込むためのデスクランブルされた識別情報を得る論理演算手段とを備えることを特徴とするものである。

## 【0006】

【作用】 かかる本発明によれば、論理演算手段によって、外部からの識別情報及びスランブルコードの間で所定の論理演算を行って、不揮発性 RAM に書き込むためのスランブルされた識別情報を得ると共に、不揮発性 RAM から読み出されたスランブルされた識別情報及びスランブルコードの間で所定の論理演算を行って、揮発性 RAM に書き込むためのデスクランブルされた識別情報を得る

## 【0007】

【実施例】 以下に、図面を参照して、本発明の実施例（例えば、デジタル方式の携帯電話機）を詳細に説明しよう。まず、図 4 を参照して、携帯電話機の一般的な回路構成を説明する。1 は送受信アンテナで、無線部 2 に接続されている。3 は制御部で、CPU 及びそれに付属する ROM 及び RAM を備えており、無線部 2 に接続されている。4 は外部インターフェースで、これより RS 232C 用外部端子 4t が導出されると共に、制御部 3 に接続されている。5 は音声部で、無線部 2 に接続され、送話器及び受話器（図示を省略）を備えている。6 は操作部で、テンキー、ファンクションキー、短縮ダイヤルキー、再ダイヤルキー等の操作キーを備え、各操作キーの操作による操作信号（キー信号）が制御部に供給される。

【0008】 次に、図 2 を参照して、図 4 における制御部 3 の一般的な回路を説明する。9 は CPU で、この CPU 9 に、パラレルバス 8 を通じて、CPU 9 の動作プログラムの記憶されたフラッシュ ROM (Flash Read Only Memory : フラッシュ・リード・オンリ・メモリ) 及び識別情報の記憶されている不揮発性 RAM としての EEPROM (Electrically Erasable Programable Read Only Memory : エレクトリカル・イレーザブル・プログラマブル・リード・オンリ・メモリ) (不揮発性 ROM) 10 が接続されている。又、EEPROM 10 及び図 4 の外部インターフェース 4 は、それぞれシリアルバス 7 を通じて、CPU 9 に接続されている。

【0009】 次に、図 3 を参照して、スランブルコード発生手段の一例としての、M 系列 (Maximum Length Code : マキシマム・レングス・コード) 発生回路の一例

を説明する。このM系列発生回路は、それぞれ1ビットの記憶素子としてのn段のレジスタ $R_1$ 、 $R_2$ 、 $R_3$ 、…… $R_n$ の縦続回路からなるシフトレジスタSRを備え、最終段のレジスタ $R_n$ から乱数出力の得られる出力端子Tが導出され、n次のM系列の乱数の生成多項式で決まる、シフトレジスタSRの所定箇所に所定個数のタップが設けられる。そして、シフトレジスタSRの最終段のレジスタ $R_n$ よりの乱数出力と、所定のタップの出力とを、エクスクルーシブオア回路 $E R_1$ 、 $E R_2$ で排他的論理和演算し、その各排他的論理和をシフトレジスタSRの初段のレジスタ $R_1$ に入力する。シフトレジスタSRの各段のレジスタの内容(1ビット)は、クロック信号によって、順次左から右に向かって転送される。かくして、出力端子Tからn次の乱数出力(オール0を除く最大 $2^n - 1$ の周期の系列)が得られる。

【0010】識別情報は、加入者番号、移動局番号、認証及び秘匿のキー等を含んでいる。乱数発生手段として、M系列発生手段を使用し、識別情報が、例えば、128バイトの場合を例にとつて、識別情報の書込み及び読出しについて、図1のCPUの機能ブロックを参照して説明する。

【0011】図1において、CPU9は、それぞれアルゴリズムに基づく、M系列発生手段9Bと、論理演算手段(ここでは、排他的論理和演算手段)9Cと、制御手段9Aとを備え、この制御手段9Aは、M系列発生手段9B、論理演算手段9C、EEPROM10、フラッシュROM11及び揮発性RAM12を制御する。

【0012】携帯電話機の製造時に、例えば、図3で説明したような外部のM系列発生回路から発生した16次のM系列乱数出力をスクランブルコードとして用い、このスクランブルコードの製品毎に、即ち、携帯電話機毎に異なる初期値を、携帯電話機に組み込んだフラッシュROM11に予め記憶するか、又は、フラッシュROM11に予め記憶したものを携帯電話機に組み込む。尚、このフラッシュROM11には、CPU9によって携帯電話機を動作させるためのプログラムも同時に記憶する。

【0013】識別情報の書込み時に、制御手段9Aの制御に基づいて、128バイトの識別情報を入力端子4tから外部インターフェース4及びシリアルバス7を通じて、CPU9の論理演算手段9Cに供給すると共に、CPU9のM系列発生手段9Bからの16次、即ち、16ビットのスクランブルコードを論理演算手段9Cに供給し、フラッシュROM11に記憶されている16次のスクランブルコードの初期値を読み出し、その初期値をパラレルバス8を通じてCPU9のM系列発生手段9Bに供給し、その初期値から開始し、識別情報の2バイト毎に更新される16次、即ち、16ビット(2バイト)のスクランブルコードをCPU9のM系列発生手段9Bから発生させる。そして、制御手段9Aの制御に基づいて、

論理演算手段9Cによってその2バイト毎に更新されるスクランブルコードと、識別情報の2バイト毎の識別情報部分との間で、排他的論理和演算を行ってスクランブルを行い、そのスクランブルされた識別情報をシリアルバス7を通じてEEPROM10に書き込む。

【0014】識別情報の使用時においては、携帯電話機の電源投入時に、制御手段9Aの制御に基づいて、フラッシュROM11に記憶されているスクランブルコードの初期値を読み出し、その初期値をパラレルバス8を通じてCPU9のM系列発生手段9Bに供給し、その初期値から開始し、識別情報の2バイト毎に更新される16次、即ち、16ビットのスクランブルコードをCPU9のM系列発生手段9Bから発生させる。そして、制御手段9Aの制御に基づいて、その2バイト毎に更新されるスクランブルコードと、識別情報の2バイト毎の識別情報部分との間で、排他的論理和演算を行ってデスクランブルを行い、そのデスクランブルされた識別情報をパラレルバス8を通じて揮発性RAM12に書き込む。又、発呼時に、CPU9の制御手段9Aの制御に基づいて、RAM12に記憶されている識別情報を読み出して無線部2に供給して、被変調信号に変換してから、アンテナ1より送信する。

【0015】このように、フラッシュROM11に記憶されたスクランブルコードの初期値は、製品毎に、即ち、携帯電話機毎に異なるものであるから、携帯電話機の制御部3のEEPROM10に記憶されているスクランブルされた識別情報を、別の携帯電話機にコピーして、実質的に携帯電話機を盗用することは不可能である。

【0016】上述の実施例では、識別情報と、M系列の乱数からなるスクランブルコードとの間で排他的論理和演算して、スクランブルされた識別情報を得、又、そのスクランブルされた識別情報と、同じM系列の乱数からなるスクランブルコードとの間で排他的論理和演算して、デスクランブルされた識別情報を得るようにした。これを一般的に表現すると、識別情報と、第1のコードとの間で、第1の論理演算を行って、スクランブルされた識別情報を得、そのスクランブルされた識別情報と、第2のコード(第1のコードとの間で所定の関係を有するコード)との間で第2の論理演算(第1の論理演算との間で所定の関係を有する論理演算)を行って、デスクランブルされた識別情報を得ることになる。この場合に、第1及び第2のコードは同じであっても、異なっても良い。同様に、第1及び第2の論理演算も同じであっても、異なっても良い。要は、スクランブルされた識別情報をデスクランブルして、元の識別情報が得られれば良い。

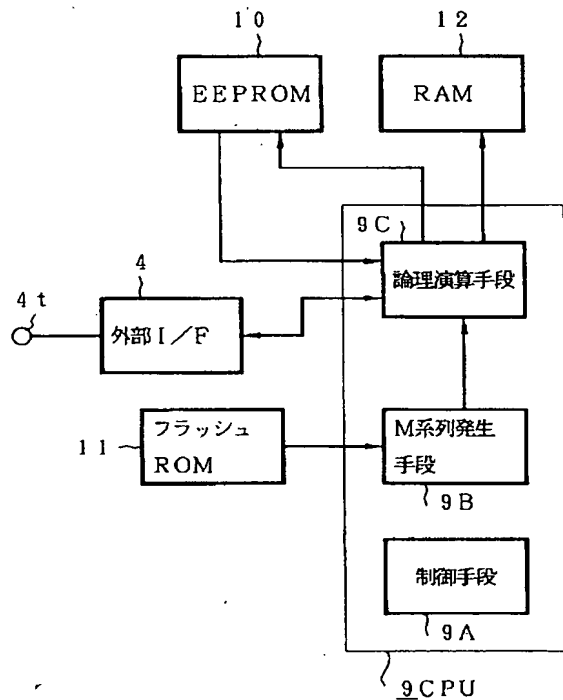
【0017】

【発明の効果】上述せる本発明によれば、スクランブルされた識別情報を記憶する不揮発性RAMと、スクラン

ブルコードの製品毎に異なる初期値が製造時に予め記憶されたROMと、デスクランブルされた識別情報を記憶する揮発性RAMと、不揮発性RAM、ROM及び揮発性RAMを制御する制御手段とを有し、その制御手段は、ROMに記憶されているスクランブルコードの初期値から順次変化するスクランブルコードを発生するスクランブルコード発生手段と、外部からの識別情報及びスクランブルコード発生手段よりのスクランブルコードの間に所定の論理演算を行って、不揮発性RAMに書き込むためのスクランブルされた識別情報を得ると共に、不揮発性RAMから読み出されたスクランブルされた識別情報及びスクランブルコード発生手段よりのスクランブルコードの間に所定の論理演算を行って、揮発性RAMに書き込むためのデスクランブルされた識別情報を得る論理演算手段とを備えるので、実質的に他人の携帯電話機を盗用することを防止することのできる携帯電話機を得ることができる。

【図面の簡単な説明】

【図 1】



CPUの機能ブロック

\* 【図 1】 実施例の制御部のCPUの機能を示す機能ブロック及びCPUの周辺回路を示すブロック線図である。

【図 2】 実施例の制御部の回路構成を示すブロック線図である。

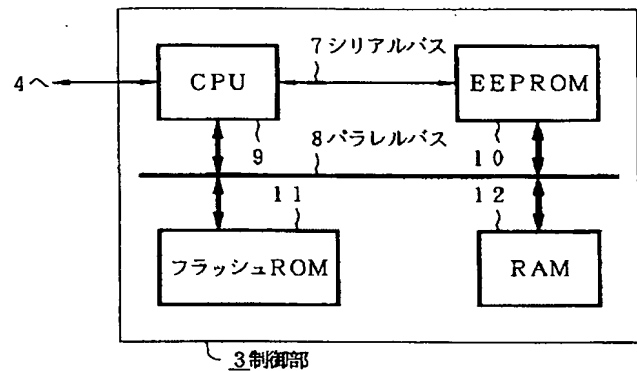
【図 3】 M系列発生回路の例を示すブロック線図である。

【図 4】 実施例の回路構成を示すブロック線図である。

【符号の説明】

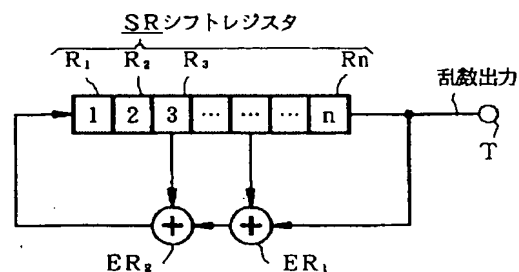
- 1 アンテナ
- 2 無線部
- 3 制御部
- 4 外部インターフェース
- 5 音声部
- 6 操作部
- 9 CPU
- 10 EEPROM
- 11 フラッシュROM
- 12 RAM

【図 2】



実施例の制御部

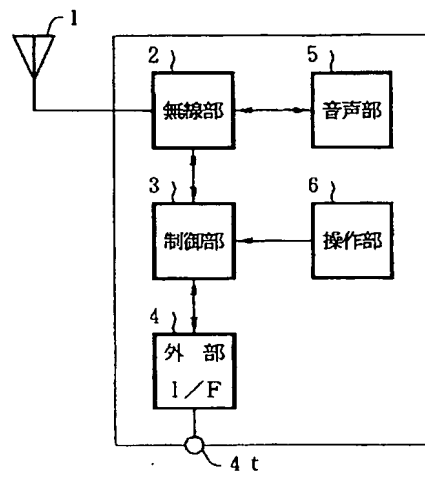
【図 3】



ER<sub>1</sub>、ER<sub>2</sub> エクスクルーシブオア回路

M系列発生回路

【図 4】



携 帯 電 話 機